



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,620	01/23/2001	Yasuyuki Murakami	81942.0013	3492

26021 7590 01/12/2005

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER

MOISE, EMMANUEL LIONEL

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/767,620

Applicant(s)

MURAKAMI ET AL.

Examiner

Emmanuel L. Moise

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 4-7,9,10,13,14,17-20,22,23,25 and 27 is/are allowed.
- 6) ☒ Claim(s) 1,8,11,12,15,16,21,24 and 26 is/are rejected.
- 7) ☒ Claim(s) 2 and 3 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 8, 11, 12, 15, 16, 21, 24 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Iwamura et al. (U.S. Patent No. 5,966,449, hereinafter “Iwamura”).

As per claim 1, Iwamura teaches the claimed secret key generating method for generating a secret key of an entity in each of a plurality of key generating agencies, comprising the steps of:

obtaining each divided identification information by dividing identification information of the entity into a plurality of blocks (column 6, lines 34-37);

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information (column 8, lines 46-48)); and generating a secret key of the entity by synthesizing the extracted components with a random number particular to the entity (column 8, lines 51-56).

As per 8, Iwamura teaches the claimed encryption method for encrypting a plaintext to be transmitted from one entity to other entity, comprising the steps of:

extracting a part of the components of a symmetric matrix of a secret for each key generating agency in accordance with each divided identification information which has been obtained by

Art Unit: 2136

dividing identification information of the one entity into a plurality of blocks (column 8, lines 46-48));

generating a secret key of the entity by synthesizing the extracted components with a random number particular to the entity (column 8, lines 51-56);

generating a common key by using a component corresponding to the other entity which is included in the secret key of the one entity (column 10, lines 5-9); and

encrypting the plaintext into a cipher text by using the generated common key (column 10, lines 49-52).

As per claim 11, Iwamura teaches the common key generating method for generating a common key which is used for an encryption process from a plaintext to a cipher text and a decryption process from a cipher text to a plaintext in a cryptographic communication between entities, comprising the steps of:

extracting components which are included in each secret key of one entity of the communication partner, each secret key being generated by using each divided identification information obtained by dividing identification information of the one entity into a plurality of blocks (column 8, lines 46-48)); and

generating a common key by using a component key by synthesizing the extracted components through XOR (column 10, lines 45-52).

Claims 12, 15, 16, 21, 24, and 26 are rejected for reasons similar to those set forth against claim 1 and/or claim 11.

Art Unit: 2136

Allowable Subject Matter

4. Claims 2 and 3 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

5. Claims 4-7, 9, 10, 13, 14, 17-20, 22, 23, 25 and 27 are allowable over the prior art of record.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

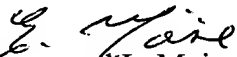
4,218,582 (Hellman et al.); 4,399,323 (Henry); 5,220,606 (Greenberg); 5,987,129 (Baba); 6,289,454 (Eslinger et al.); and 6,298,137 (Hoffstein et al.).

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Emmanuel L. Moise whose telephone number is (571)272-3865. The examiner can normally be reached on M-W (9:30-6:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Emmanuel L. Moise
Primary Examiner
Art Unit 2136